Chapter XXVI

Business Continuity and Disaster Recovery Plans

Yvette Ghormley
Saint Leo University, USA

ABSTRACT

This chapter describes the tools that businesses can use to create a Business Continuity and Disaster Recovery Plan. Utilizing business modeling, business impact analysis, risk analysis, and mitigation strategies, businesses can analyze their operations to learn the business critical functions that must be recovered as quickly as possible during any type of disaster. These processes are illustrated using the case study of a hypothetical small manufacturing business located in California. Specific information technology solutions are also discussed and the necessity of integrating them into the overall plan. Businesses that are prepared to face any kind of disaster with an implemented and tested Business Continuity and Disaster Recovery Plan are much more likely to survive than businesses that do not have such a plan. It is hoped that the contents of this chapter will spur business owners that have not yet adopted such a plan to do so.

INTRODUCTION

Disasters have affected businesses in all shapes and forms for hundreds of years. However, with the advent of high-speed communication, computers, digitized data, and vastly increased reliance on databases and electronic storage of information, businesses have a lot more to lose than hardware if a disaster strikes. Many businesses also operate in a “24/7” environment and are global in their scope of operations. A high percentage of small businesses are also Internet-based, or have a significant portion of income derived from the Internet, a marketing and selling resource system that 15 years ago was little more than a curiosity.

Consider the following facts: (a) 80 percent of businesses affected by a major “incident” close within 18 months, (b) 90 percent of businesses that lose data as a result of a disaster close within two years, and (c) 58 percent of UK businesses were disrupted by a manmade disaster over 3,000 miles away in another country (the World Trade Center terrorist attacks of September 11, 2001 in New York) (Taylor, 2006). It is clear that all businesses, from large multinational corporations down to the “mom and pop” business selling services on Internet, must develop a disaster recovery (DR) plan and prepare for business continuity (BC) following an incident that affects business operations.

It used to be that BC and DR plans were the domain of IT departments, and while some of the mission-critical items are certainly IT-related, the functions of IT must be integrated into the overall plan (Taylor
D’Amico (2006) recommends a three-pronged approach to preparing BC and DR plans. First, the Resolve Phase, which involves assessing the risks, whom should be involved, what units of the business are most critical, and what steps can be taken to minimize risk. Second, the Respond Phase, which includes formation of the disaster response team, how information will be disseminated to employees, how customers and suppliers will be notified, and where personnel will operate and with what equipment. Third, the Rebuild Phase, which includes the decision of which personnel will be directly involved in damage assessment and rebuilding, adjustments to business operations while rebuilding is in progress, and the maintenance of operations so that business can proceed. This is the approach adopted for the chapter.

The chapter comprises four main sections: (a) background, which includes categories of disasters that can impact businesses, consequences, and an outline of business continuity and disaster recovery methodologies; (b) the three-phase approach to BC and DR, which includes (1) constituting a BC & DR team, (2) assessing the risks of likely disasters, (3) forming a priority list of business-critical functions, (4) mitigating the risks, (5) creating operations plans in the event of a disaster, (6) writing the BC & DR plan in simple manual form, (7) implementing and testing the plan, and (8) specific IT and engineering functions that must be integrated into the overall plan, which include backup and distribution of company data and records, provision of hardware and software backup, specific supplier and intercompany agreements, satellite and voice-over IP (VOIP) telephone switching, utility backup, temporary employee and business relocation, and restoration of critical systems on a priority basis; (c) future trends; and (d) conclusions.

The chapter will be most geared toward small and medium-sized businesses and entities.

BACKGROUND

Types of Disasters

Several descriptors exist that can help define a disaster from the point of view of a business. The first is the scale or geographic footprint. An onsite disaster is one that only affects a business’ operations at a given location. A denial-of-service attack aimed at a company’s servers, or the broken water pipe that showered a Pennsylvania hospital’s data center (Buckley, 2002) are both examples of this category. The next higher level is the local disaster, which typically affects a community. For example, a fire that damaged a main communications cable in Manchester, England on March 29, 2004 left 130,000 homes and businesses without phone or Internet services (Taylor, 2006). Higher still is the regional-level disaster, typified by Hurricane Katrina, whose damaging winds and resultant storm surge caused 1,570 deaths in Louisiana and $40-50 billion in economic losses (Kates, Colten, Laska & Leatherman, 2006). At the highest level of the scale are national and international disasters. If the H5N1 influenza strain ever develops into a pandemic, this will be one unwelcome example (Maldin, Inglesby, Nuzzo, Lien, Gronvall, Toner, et al., 2005).

The second is the type of disaster: manmade or natural. Earthquakes, floods, hurricanes, and tornadoes, are examples of the latter, while the attacks of September 11, 2001 or the Phillips Petroleum chemical explosion in Pasadena, Texas, exemplify the former. However, there can also be a gray area insofar as the impact of a natural disaster can be far larger when inappropriate risks or actions are taken. Thus one might argue that the flooding of New Orleans after the passage of Hurricane Katrina was a result of poor levee maintenance, rather than an exceptionally severe hurricane.

The third parameter is the duration of the initial event that constitutes the disaster. Usually this is measured in minutes or hours, but certain incidents, such as flooding or snowstorms, can have durations of several days or even weeks.

The final descriptor is whether any warning occurs, and the length of the warning preceding the disaster. Most disasters have little or no warning, although there might be useful imminent signs, particularly with natural disasters, that are probability-related.

Occasionally, disasters can occur that have more of a diffuse geographic nature, but which nevertheless still impact business. Coombs (2004) lists several examples that do not fit the classic disaster profile, such as product tampering (e.g., the Tylenol tampering cases involving cyanide), a technical error accident, which can be exemplified by the crash of an airliner, or a technical error recall, such as a product failure in the marketplace.